BAB I
PENDAHULUAN

1.1 Latar Belakang

Keamanan jaringan merupakan hal yang sangat penting untuk diperhatikan, terutama pada teknologi jaringan komputer sangat pesat pada era sekarang ini. Banyak orang maupun institusi telah menerapkan sistem informasi yang tidak lepas dari jaringan komputer. Demikian juga ancaman keamanan sistem jaringan juga berjalan seiring perkembangannya. Dalam sistem jaringan pasti ditemui kekurangan yang sering muncul,diantaranya adalah gangguan dari dalam berupa virus atau jaringan komputer yang bermasalah dan gangguan dari luar bisa berupa semua bentuk *attacking network system* [1].

Gangguan sistem jaringan dari dalam bisa saja karena ada otoritas yang menghendaki perbaikan sistem ataupun pengolahan data sistem sehingga meninggalkan gangguan berupa *virus* ataupun koneksi yang *down*, akan tetapi gangguan dari luar adalah tindakan diluar otoritas yang tujuannya lebih pada perusakan dan pencurian data. Serangan dari luar diantaranya adalah *Buffer overflows, DDoS attack, CGI attack, SQL injection, Port Scanning ,FTP brute force dsb.*Semua serangan ini bersifat merugikan, karena informasi yang seharusnya menjadi sangat tertutup bisa diambil oleh yang tidak bertanggung jawab.Serangan-serangan tersebut juga masih sangat berpotensi besar untuk berkembang dan semakin bervariasi.Oleh karena itu diperlukan solusi untuk menangani serangan yang semakin berkembang ini [2].

Dengan menggunakan *Intrusion Detection System (IDS) snort* merupakan salah satu solusi untuk menangani serangan-serangan tersebut, Snort merupakan aplikasi *open source* yang dapat berjalan dengan baik di banyak *platform*,salah satunya pada sistem operasi linux . Dalam penelitian ini penulis akan merancang *sistem monitoring* keamanan jaringan yang akan mendeteksi serangan-serangan yang masuk pada jaringan yang terhubung pada server linux,sehingga seluruh paket yang masuk kedalam jaringan

tersebut.Setelah itu akan memberi informasi berupa telegram *messages* kepada *administrator* jaringan bahwa telah terjadi sebuah serangan.Dengan menggunakan metode pengujian yaitu penetration test dimana pengujian secara langsung menggunakan simulasi serangan jaringan pada instansi terkait.

Pada Telegram Bot merupakan akun Telegram khusus yang dirancang untuk ini msecara otomatis memproses pesan. Pengguna dapat berinteraksi dengan bot mmengirim pesan perintah (*Command*) melalui pesan pribadi atau group.Akun Telegram Bot bertindak sebagai antarmuka pengguna untuk menjalankan kode di server. Misalnya, Bot Telegram dapat dibuat sesuai permintaan digunakan dengan mengintegrasikannya dengan layanan lain Bangun rumah pintar, layanan sosial, buat alat khusus atau melakukan segala sesuatu secara virtual [3].

SMK Pancasila 8 Slogohimo adalah sekolah menengah kejuruan yang terletak di JL.RAYA SLOGOHIMO-WONOGIRI, Slogohimo, Kec.Slogohimo, Kab.Wonogiri, Prov.Jawa Tengah. SMK Pancasila 8 Slogohimo memiliki laboratorium yang digunakan untuk proses belajar mengajar.Tentu saja banyak data-data penting yang terdapat pada server laboratorium tersebut. Perlu pengawasan pada server laboratorium supaya tidak terjadi kebocoran data ataupun pemasukan paksa serta kerusakan yang dilakukan oleh orang yang tidak bertanggung jawab.

Berdasarkan masalah dan tinjauan diatas penulis mengambil sebuah judul **"Sistem Monitoring Keamanan Jaringan Menggunakan IDS Snort Dengan Bot Telegram Di SMK Pancasila 8 Slogohimo".**Sehingga tujuan dari penelitian ini adalah memberi solusi apabila terjadi adanya serangan pada jaringan khususnya untuk jaringan *LAN* di Laboratorium SMK Pancasila 8 Slogohimo lewat pendeteksian.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan sebelumnya, maka masalah dari penelitian ini adalah sebagai berikut:

1. Bagaimana melakukan implementasi *Intrusion Detection System (IDS)* Snort menggunakan sistem operasi linux Ubuntu 22.04 *LTS* di server laboratorium SMK Pancasila 8 Slogohimo?
2. Bagaimana mengidentifikasi adanya serangan jaringan yang ada di lab komputer SMK Pancasila 8 Slogohimo menggunakan *Intrusion Detection System (IDS)* Snort dengan bot telegram?

1.3 Batasan Masalah

Dalam pembuatan skripsi ini penulis membatasi masalah yang akan dilaksanakan, sebagai berikut:

1. Server menggunakan sistem operasi Linux Ubuntu 22.04 *LTS*.
2. Jaringan yang diuji hanya lingkup laboratorium di Smk Pancasila 8 Slogohimo.
3. Menggunakan tools *IDS Snort*.
4. Server hanya melakukan pemantauan dan memberi notifikasi ke Administrator melalui aplikasi telegram.
5. Serangan yang digunakan adalah *DDoS attack(TCP, UDP Syn flood attack),port scanning ,ICMP*
6. Bot telegram hanya sebagai media notifikasi jika ada serangan.
7. Dalam skripsi ini peneliti tidak melakukan implementasi peningkatan keamanan jaringan yang sudah ada. Melainkan memberi solusi terhadap adanya serangan jaringan.

1.4 Tujuan Penelitian

Manfaat penelitian yang dihasilkan dari penelitian ini adalah:

1. Dapat melakukan implementasi *Intrusion Detection System (IDS)* Snort menggunakan sistem operasi linux di server Lab. komputer Smk Pancasila 8 Slogohimo
2. Dapat melakukan analisa sistem monitoring pada server linux Ubuntu 22.04 *LTS*.
3. Dapat memahami cara kerja *IDS Snort*.
4. Menganalisis jaringan *LAN* menggunakan tools dari *IDS snort*.

1.5 Manfaat Penelitian

Manfaat penelitian yang didapat dari hasil penelitian adalah:

1. Bagi Objek
    a. Memberikan solusi terbaik bagi keamanan jaringan di sekitar lab kompuer Smk Pancasila 8 Slogohimo
    b. Membantu pihak administrator untuk mengawasi keamanan jaringan dan server dari bahayanya serangan
2. Bagi Penulis
    a. Memahami tentang merancang sistem monitoring keamanan jaringan berbasis linux
    b. Membuat sebuah karya tulis yang bermanfaat
3. Bagi Pembaca
    a. Sebagai bahan pembelajaran
    b. Untuk referensi

1.6 Sistematika Penulisan

Dalam penulisan ini, penulis membuat suatu sistematika yang bertujuan untuk menggambarkan secara ringkas bab-bab yang mencakup hal-hal sebagai berikut:

1.6.1. BAB 1 PENDAHULUAN

Bab ini berisikan mengenai latar belakang, rumusan masalah, batasan masalah tujuan penelitian, manfaat penelitian dan sistematika penulisan.

1.6.2. BAB II TINJAUAN PUSTAKA

Bab ini berisi penjelasan tinjauan pustaka yang digunakan diantaranya konsep dan teori serta perangkat lunak untuk merancang sistem monitoring pada penelitian ini. Pembahasan dalam tema penulisan ini yang didapat dari beberapa literatur dan e-book.

1.6.3. BAB III METODE PENELITIAN

Bab ini berisi berupa rancangan dan desain sistem yang akan digunakan untuk penelitian.

1.6.4. BAB IV HASIL DAN PEMBAHASAN

Bab ini berisi mengenai penjelasan tahapan perancangan sistem, implementasi metode hasil testing dan pembahasan.

1.6.5. BAB 5 PENUTUP

Bab ini berisi penjelasan mengenai kesimpulan dan saran yang diperoleh dari pembahasan pada bab sebelumnya